This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Previously Presented) A method for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices, comprising:

providing an association of at least one coding key to the plurality of storage cartridges;

encrypting the coding key;

receiving, by the interface devices, an Input/Output (I/O) request;

decrypting, by the interface devices, the encrypted coding key in response to the I/O request to use to decode data to be read and code data to be written with respect to the storage medium of at least one of the storage cartridges to perform the received I/O request.

2. (Original) The method of claim 1, further comprising:

using the coding key to encode data to write to the storage medium;

transmitting the encoded data to the interface device to write to the storage medium in one storage cartridge mounted in the interface device;

receiving encoded data from the interface device read from the storage medium; and

using the coding key to decrypt the received encoded data.

3. (Previously Presented) The method of claim 1, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

4. (Original) The method of claim 1, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

5. (Original) The method of claim 1, wherein the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge.

6. (Original) The method of claim 1, further comprising:

transmitting the encrypted coding key to the interface device, wherein the interface device decrypts the coding key to use to decode and code data stored in the storage medium.

7. (Previously Presented) The method of claim 6, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein the interface devices use a second key to decrypt the coding key encrypted with the first key.

8. (Previously Presented) The method of claim 6, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein a second key is used to decrypt the coding key encrypted with the first key;

encrypting the second key with a third key, wherein the interface devices uses a fourth key to decrypt data encrypted with the third key; and

transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device.

9. (Previously Presented) The method of claim 6, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein a second key is used to decrypt the coding key encrypted with the first key;

transmitting the coding key encrypted with the first key to the interface device;

receiving, from the interface device, the coding key encrypted with the first key;

decrypting the coding key with the second key;

encrypting the coding key with a third key, wherein a fourth key is used by the interface device to decrypt data encrypted with the third key; and

transmitting the coding key encrypted with the third key to the interface device.

10. (Previously Presented) A method performed by an interface device for accessing data in a removable storage cartridge including a read/write storage medium coupled to the interface device, comprising:

receiving an encrypted coding key from a host system with an Input/Output (I/O) request;

decrypting the encrypted coding key;

using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request;

using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and

storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

11. (Original) The method of claim 10, wherein encoding the data with the coding key compresses the data and wherein decoding the data written to the storage medium decompresses the data, and wherein the data can only be encoded or decoded using the coding key.

12. (Previously Presented) The method of claim 10, wherein the coding key is encrypted by a first key maintained at the host system, further comprising;

maintaining a second key to decrypt data encrypted using the first key, wherein the second key is used to decrypt the coding key encrypted with the first key.

13. (Original) The method of claim 12, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

14. (Original) The method of claim 13, further comprising:

transmitting the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

15. (Original) The method of claim 12, further comprising:

storing the coding key encrypted with the first key within the storage cartridge;

receiving an input/output (I/O) request directed to the storage cartridge; and

accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

16. (Previously Presented) The method of claim 10, wherein the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key, further comprising:

receiving, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the host system; and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

17. (Previously Presented) The method of claim 10, wherein the coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key, further comprising:

transmitting the encrypted coding key received from the host system back to the host system; and

in response to transmitting the encrypted coding key back to the host system, receiving, from the host system, the coding key encrypted using a third key, wherein data encrypted using the third key is decrypted using a fourth key; and

accessing the fourth key, wherein the coding key is decrypted using the fourth key.

18-43. (Canceled)